

Continuity Strategy Planner

Disaster Risk Management Authority | The Bahamas

Derived from the DRM Authority Business Continuity Planning Workbook

What this tool helps you do

Turn priority vulnerabilities into practical continuity arrangements that can keep a critical activity operating, allow it to operate temporarily at a reduced level, restore it within the required timeframe, or provide an alternative until normal operations return.

Use this tool when...

- you have identified critical functions and recovery priorities;
- you know the main dependencies, vulnerabilities or single points of failure affecting those functions;
- an existing backup or alternative is weak, untested or missing; or
- you need to decide what should happen if normal operations are disrupted.

How to use the tool

1. Select the vulnerabilities that could most seriously interrupt a critical function.
2. Identify a risk-reduction measure and a practical backup or alternative.
3. Record what must be arranged before disruption occurs.
4. Decide the minimum level of operations the business must preserve.
5. Set clear activation triggers and decision authority.
6. Confirm the priority strategies, owners and advance actions.

Key concept

Continuity Strategy

A continuity strategy is the practical arrangement used to keep a critical activity operating, operate it temporarily at a reduced level, restore it within the required timeframe, or provide an alternative until normal operations return.

Strategy areas to consider

People

Cross-training, documented procedures, alternate decision-makers, remote work, temporary reassignment, contractor support, flexible work, backup system access.

Premises

Remote work, another branch, temporary rented/shared space, partner premises, mobile operations, online service, reduced operations.

Utilities

Electricity, water, Internet, mobile service and payment systems: identify the backup, how long it can support the business and what improvement is needed.

Technology & Data

Automatic backups, cloud or off-site copies, alternative devices, secondary Internet access, manual processes, documented restoration, authorized backup users.

Suppliers

Identify alternatives, how quickly the business could switch, and whether the alternative is vulnerable to the same disruption as the primary supplier.

Financial Continuity

Consider payroll, supplier payments, emergency purchases, banking access, insurance claims, cash/liquidity and financial records.

1. Continuity Strategy Planner

Start with the priority vulnerabilities identified in your dependency and vulnerability analysis. For each one, identify a practical way to reduce the risk, a backup or alternative, and what must be put in place before a disruption occurs.

Priority Vulnerability	Critical Function Affected	Risk-Reduction Measure	Backup / Alternative	What Must Be Arranged in Advance?

Questions to test each proposed strategy

Practical

Can the business realistically use this arrangement during the disruption we are planning for?

Timely

Can it be activated quickly enough to support the Target Recovery Time for the critical function?

Independent

Could the same disruption disable both the primary arrangement and the backup?

Accessible

Can the right people access the systems, premises, funds, information or authority needed to use it?

Sustainable

How long can this arrangement support the business before another option is needed?

Resourced

What people, equipment, suppliers, money, contracts, access or approvals must be arranged in advance?

Owned

Who is responsible for putting the arrangement in place and keeping it current?

Tested

How will the business confirm that the strategy works before it is needed?

2. Minimum Viable Operations

Continuity does not always mean restoring the entire business immediately. Sometimes survival depends on operating at a reduced level. Identify the services that must continue and the minimum resources needed to sustain them.

Most Important Service / Function to Continue	Minimum Level We Need to Maintain	Minimum People / Resources / Arrangements Needed

Services or activities we could temporarily suspend: _____

3. Strategy Activation Triggers

A strategy should be activated when a defined condition occurs. Identify the condition or threshold that will signal when each priority strategy should be activated, and who has authority to make that decision.

Strategy	Trigger / Condition	Who Makes the Decision?

Example trigger

If the primary supplier cannot deliver within 48 hours, the trigger may be to contact the alternate supplier. The important point is to decide the threshold and authority before the business is under pressure.

4. Priority Continuity Strategies

Select the three strategies that matter most to protecting or restoring your critical functions. Confirm what each strategy addresses, what will be done, who owns it and what must be arranged before it is needed.

Priority Strategy 1	What Will We Do?	Owner	What Must Be Arranged?
Vulnerability addressed:			
Critical function affected:			

Priority Strategy 2	What Will We Do?	Owner	What Must Be Arranged?
Vulnerability addressed:			
Critical function affected:			

Priority Strategy 3	What Will We Do?	Owner	What Must Be Arranged?
Vulnerability addressed:			
Critical function affected:			

What to do next

Carry these priority strategies into your Business Continuity Plan. Confirm the related activation triggers, decision authority, resource requirements and owners, then test the arrangements before relying on them. For the complete planning process, see the DRM Authority Business Continuity Planning Workbook, Section 4: Continuity Strategies.

Use and Reproduction Notice

Version 1.0 | September 2026

This tool has been developed by the Disaster Risk Management Authority (DRM Authority) of The Bahamas as part of its Business Resilience Programme and is provided to support practical business continuity and resilience planning.

Businesses and organizations may reproduce and adapt this tool for their own internal business continuity and resilience planning, provided that attribution to the DRM Authority and any applicable third-party acknowledgements are retained.

This tool, its templates, or any substantial portion of them may not be sold, rebranded, republished, incorporated into a commercial product, or used to deliver paid training, facilitation, consultancy or other commercial services without the prior written permission of the DRM Authority.

Use of this material does not imply endorsement, accreditation or certification by the DRM Authority. Third-party material, where identified, remains subject to the rights and terms of its respective owner.

Internal adaptation is permitted. Commercial reuse requires prior written permission.